Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment
Version 1.3

Security Policies in a Global Organization

By: Gerald P. Long

ABSTRACT

In a global organization, special difficulties arise in creating and maintaining effective information security policies. Difficulties include varying risk tolerance levels among business units, legal and business cultural differences and policy differences arising through merger or acquisition. In order to deal with these issues, it is probably necessary to create a tiered structure of information security policies with some policies applying globally throughout the organization, and other policies applying to individual geographical, or regional entities.

An important factor in deciding where to draw the line between global and regional information security policies is the nature of the organization's communication network. If the network is centrally managed or tightly coupled, global policies should be developed for some topics, since the attacks on information security could move along the network from region to region. Some issues may require region-specific policies that may be more restrictive than global policies, but cannot invalidate the global policies.

The approval structure for tiered information security policies should parallel the structure of the policies themselves, i.e. if the policies are tiered, then a tiered approval structure is necessary.

1. Why Have Information Security Policies?

Webster defines "policy" as "a high-level overall plan embracing the general goals and acceptable procedures." It is generally accepted that an organization's information security policies should be the basis for its information security program. Especially in the case of global organizations, the need for sensible policies and the problems inherent in creating them are very significant. This paper discusses the some of the special information security policy-related issues that are common among global organizations, and offers some ways to resolve them. Some of the issues discussed may apply also to organizations without a global presence.

Despite common agreement among information security professionals, auditors and others in control-oriented disciplines, information security policies do not come into being

in many organizations, global or otherwise, until forced by one of the following external causes:

- An audit finding that the information security program is inadequate and needs a new set of policies.
- A security incident, such as loss of a computer, a hacking incident, costly downtime due to a computer virus, or similar occurrence.
- Pressure form a regulatory body.
- Insistence by customers or business partners that your information security program conform to standard industry practice.
- A senior management change, with the new management recognizing lack of controls as a possible cause of inefficiency.

1.1 What Is A Global Organization?

For our purposes, a global organization will have several of the following characteristics:

- A presence on multiple continents,
- A presence in several countries, subject to varying laws and regulation,
- Multiple corporate entities tied together under some form of organizational umbrella;
- Diverse local business environments and cultures among its varying entities,
- A history of growth through acquisition, bringing together organizations with contradictory security and other management
- Diverse information technologies, implemented with inconsistent information security models.
- Varying levels of understanding of management and organizational controls and standard information security practices.
- Conflicting business goals and objectives among the regional business units based on local market dynamics and local business culture.

All of these factors make it very difficult to define and adhere to a coherent set of information security controls and policies in a global organization. It is more necessary than ever to find a way to implement the right information security policies at the right level, and to base the deployment of global information technology solutions on these policies. Many global organizations have global brand identities leading customers to expect the same levels of service and performance wherever they are in the world. This includes consistent protection of customer privacy, and protection against fraud, regardless of which part of the global organization is involved in a business transaction.

Against the backdrop of these global needs, there are region-specific needs that may be even more stringent than the global security requirements. A tiered set of information security policies is probably part of the answer.

1.2 Definitions

For purposes of this paper, the following definitions will be used for the components making up a global organization:

- Global organization – The organization as a whole, consisting of a center and all of the subordinate regions.
- Center – The parent or governing entity
- Region - Any entity subordinate to the Center that is part of the global organization. Regions are independent vis-à-vis one another.

1.3 Issues Affecting Global Information Security Policies

Legislation

Different regions in a global organization may be governed by conflicting legislation. An example of this is in the area of privacy legislation, discussed in greater detail below.

Another example of the effect of conflicting legislation may be in access control to information resources. It is customary in the United States to require that thorough background checks be performed before a new employee is granted access to confidential information, but such background checks may be illegal under laws in some Asian countries. The global organization can adopt the least-common denominator policy to be consistent, or it may make sense to have different policies among its regional entities.

The Internet

The growth of the Internet as a means of conducting global business highlights the need for rational, coherent information security policies in the face of diverse contradictory business culture and practices. The rise of corporate extranets, with external users throughout the world requires that security policy consider the worldwide security issues. The need to exchange electronic information among entities in a global organization mandates that varying legislative, cultural and local business issues be rationalized among the organizations to produce consistent global information security policy for email service.

Threats to a corporate IT infrastructure come may come from terrorist organizations in other countries (cyber-terrorism) or from misdirected individuals just interested in feeling powerful by disrupting business through viruses or other means (cyber-hooliganism). Since these threats may originate anywhere in the world and move quickly through an organization's global network, global

solutions are necessary. These must be based on consistent global policy. If virus protection policies are inconsistent, so will the virus protection solutions be inconsistent, and losses due to viruses may be excessive.

Culture

Within a global organization, there are likely several distinct business cultures and organizations operating with possibly conflicting management styles. These cultures may exist as subsets of the national culture where each entity is located, or may derive from the nature of the business itself. It makes no sense to write policies so strictly that not all organizations can afford to comply. An isolated organization, with minimal technology, not connected to corporate network resources will still have a very real need for an information security policy. That policy, however, will be very different from the policies required by the rest of the organization, which may be very technology-dependent, using global network technology, connected to the internet, exchanging electronic information with business partners, etc.

2. Global Information Security Policy Requirements

Global Information Security Policies should meet the following objectives:

- Information security policies should be consistent with each organization's willingness to accept risk.
- Global information security policies need to be in place if networks and technology cause a risk in one region to be shared globally throughout the organization.
- It may be necessary to have regional-specific policies to address legislative restraints, or to deal with region-specific risks that are not shared.
- Information security policies must be supported by a global approval structure that gives adequate representation to all stakeholders, and parallels the organizational structure of the policies themselves.

Ideally, most policies will be global in scope, with regional policies devoted to exceptions or extensions to meet specific regional needs.

3. Some Considerations Before You Start

3.1 Review Existing Information security Policies

Gather all instances of existing information security policy throughout your global organization and analyze them to understand what policies are in effect, whether they are consistent, and whether they make sense. In many cases, you will find that the policies

are out of date, written inconsistently, that they are largely ignored, and that many employees are unaware of them.

3.2 Headquarters Vs Regional Entities – Where To Begin?

Ideally, development of global information security policies will be initiated from the center headquarters organization, but that may not always be where the initial impetus arises. If you are in a region and cannot get a project started by the headquarters organization, what should you do? The safest approach is to tackle the policies at the region-specific level, with hope of setting a standard that can be extended globally at a later date with modifications if appropriate.

3.3 Consistency With Other Policies

Even if you do not have formal information security policies, your organization probably already has a number of policies in force that may affect information security. Obtain copies of all of these policies if possible. Some policies that you should review thoroughly are listed below.

Physical Security Policy

Your organization may have a physical security policy dealing with such topics as employee safety, physical badging and identification, building security, and employee safety. You should review this policy carefully and decide whether it will satisfy the needs for physical security of IT facilities. If it does, do not include redundant information in the information security policies you develop. If the policies do not adequately address physical security of IT facilities, you should either request that the physical security policy be updated, or include this topic in the scope of the new information security policies to be developed.

Personnel Policy

Your organization probably has a Personnel policy, and perhaps multiple Personnel policies throughout subordinate regional entities. These policies probably include hiring rules, including background checks for new employees, temporary workers, contractors, vendors or consultants. Do not recreate this language in the information security policy set. If the policy is inadequate for information security purposes, try to have it strengthened.

Another part of the personnel policy may describe progressive disciplinary actions, including discharge for misconduct. You must ensure that the information security policy is consistent with this policy provision. Do not replicate this language in information security policies. It is likely that the progressive discipline policies among geographic entities.

3.4 Use A Prewritten Set Of Policies Or A Template?

Unless your global organization has had a wholesale policy rewrite in the past few years, you will have a decision to make early on in your project: "Should we revise the existing policies, or should we develop an entirely new set of policies?" For this paper, assume that you decide that it will be too difficult to salvage the existing policies. Therefore, a new set of policies must be created. The existing set of policies can still be used as a check to ensure that no controls are dropped without proper consideration.

The next question is whether to build a set of policies from scratch or to use some form of prewritten policies as a guide. In most cases, it will be smarter and more efficient to start with a full set of policies, or a template, rather than a blank sheet of paper. This, of course, depends on the quality of existing policies, and whether they meet the global and regional needs. There are several reasons for this, including the following:

- If you build from scratch, how will you be sure that you have covered all bases and provided all necessary controls? Why not gain leverage from the work already done by others.
- If you are an organization needing to be certified as compliant with a control standard, such as the ISO 17779 standard, then the decision is easy, you need to customize the ISO 17779 template.

Note that it is unlikely that any single prewritten set of policies will apply exactly to the specific requirements caused by your organization's global structure. Most of the prewritten policy sets assume a monolithic set of security requirements. You will still need to adapt the template to your global requirements.

ISO 17799

ISO 17799 is a comprehensive set of information security policies maintained by the Information Standards Organization, and based on an earlier standard, BS7799. It can be thought of as the holy grail of information security standards, and can be used minimally as a standard against which to measure the policies that you develop, even if you do not endeavor to implement the entire standard. In European Union (EU) countries, the standard is more widely embraced than in the United States. Implementing the full set of policies encompassed in ISO 17799 is a daunting task, and one which may be hard to justify to senior management of many organizations, unless driven by an external force such as an unfavorable audit, pressure from a regulatory body, or pressure to match the competition.

In any case, the full standard can be downloaded for a relatively modest charge.

Total cost of all of the piece-parts of the standard will be less than $1000.

Other Prewritten Policy Sets

A number of other full sets of policies can be purchased on the Internet. The SANS Institute offers individual topical policy templates. Check the references at the end of this paper for some web links to sites that offer information security policy templates or sets.

Consulting Firms

If you lack time and staff to develop a set of policies, a number of major consulting organizations have developed practices to assist in creating a set of information security policies. You will become quickly aware that this is probably the most expensive way to implement a set of policies, but for some organizations it may make sense to do so. Reasons include the following:

- A very healthy budget
- Lack of staff, or a very tight deadline
- A culture that will not respect the policies unless they are developed by credentialed outsiders.

If an outside consulting firm is employed, remember that you will still have to direct their work and make all of the key decisions as to which policies to adopt, and at what level to deploy them.

4. Tackling the Global Issues

In general, global information security policies will define the minimum set of rules needed to bind the organization together and enable any entity to do business anywhere in the world. Region-specific policies will tend to be more restrictive, in reaction to more specific requirements. This should be kept in mind when evaluating policy changes. Remember, global policies are general, regional policies are more specific and restrictive. Some of the issues to be encountered are listed below.

4.1 Technical Considerations May Require Strong Central Policies

Does your organization have a single network, separate networks for each region, or something in between? Are parts of the global network outsourced? If separate networks exist, are they insulated from one another? These are important considerations in deciding whether the information security policies you develop will apply to the global organization, or to only one or more of the global entities. Such issues may be difficult for non-technical region-specific managers to understand, since they may have a charter to act independently in response to local market conditions. If the network is closely connected with headquarters network, e.g. a single domain for email messaging, it will not be possible to have completely independent regional information security policies. A

common reaction of region-specific management is to "assume the risk" of not having strong policies. Based on the way the network is designed, however, a risk taken by one organization will probably be shared throughout the global organization. This issue is probably the most important one to deal with in deciding the issues of global vs. regional information security policy.

4.2 Varying Laws Or Government Regulations Affect Your Policies

If your organization is subject to laws or government regulation in one or more jurisdictions, your information security policies will need to reflect this. In general there are two approaches. One approach is to make the policies uniform and compatible with the most restrictive set of regulatory requirements. Then, cross-regional transactions with customers will be compliant to any set of local laws. An example of this is the need of US-based organizations to adopt privacy policies that consider the legal and regulatory requirements of European Union (EU) countries. Adopting ubiquitous strong policies for all entities may drive up costs of doing business where these costs could be avoided legally by lest restrictive policies.

Another example, which goes in the other direction, involves pre-employment background checks. These checks are routine and common in some form in the United States. In some countries in Asia, such checks are illegal. In this case, policies may need to vary by region.

A third example is the fact that encryption is illegal in some middle eastern countries, which will invalidate a global policy mandating encryption of sensitive data when it is stored or transmitted.

4.3 Regional Autonomy Will Affect Global Policies

Your organization may have a management structure that declares each region to be an independent business unit. The region units may be geographically based, or serve separate distinct markets in the same country or continent. Regardless of whether such management autonomy has been granted, you may need global policies anyway. This will likely be a surprise to regional management, and poorly received. If two regions share a network or use application systems jointly, common information security policies are necessary to provide a common information security foundation for both organizations.

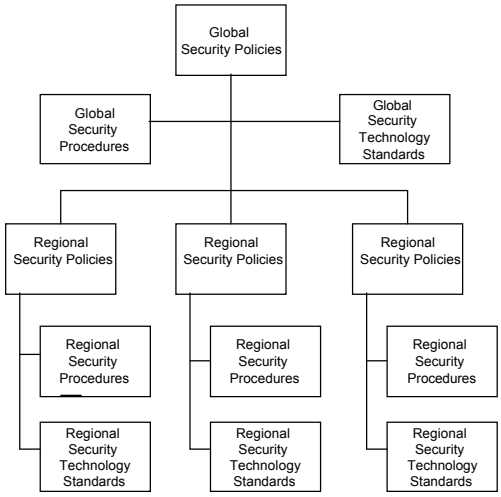
4.4 Mergers And Acquisitions Complicate The Situation

Beginning in the 1990s, we witnessed a rapid consolidation of businesses. The number of banks has shrunk, as large banks gobbled up their mid-tier competition. Large conglomerates became even larger, through merger and acquisition. Time Life merged

with Warner Brothers, and Time-Warner subsequently merged with America Online.

What does this do to the information security policies of the resulting organizations? There is no uniform answer. The most important consideration is whether the telecommunication networks became tightly coupled. Another consideration is whether there was an attempt to merge the cultures of the organizations.

5. Generalized Global Information Security Policy Structure



Above is a schema that can be used to provide structure to information security policies in a global organization. This schema is a generalized model that will vary according to the complexity of the global organization. Definitions of the various boxes follow:

Global Security Policies

Global Security Policies refer to the set of rules and practices applied to the entire global organization to regulate security over its information resources. These policies only address issues for which the organization has agreed that a global solution is required. Ideally, most policy will be written at this level.

Global Security Procedures

Global Security Procedures assist in complying with applicable global security policies. They will be followed by all entities in the global organization.

Global Security Technology Standards

Global Security Technology Standards specify a minimum baseline for uniform use of specific security technologies that are global in their application throughout the organization. They specify how a technology is to be configured, maintained

and operated, regardless of where it appears in an organization. These standards help ensure that global security policies are followed uniformly.

Regional Security Policies

Regional Security Policies refer to the set of rules and practices applied to the region organization to manage its information resources. Regional policies must not contradict global policies, and exist only where Regional diversity is appropriate.

Regional Security Procedures

Regional security procedures relate to Regional security policies as global security procedures relate to global security policies.

Regional Security Technology Standards

Regional security technology standards exist where to support Regional security policies, or in cases where there are circumstances that make it impossible to follow the global standard, even if there is no specific regional policy. For example, a region may not have available all of the technology available in the United States or Europe. TCP/IP technology may be deployable in one part of the world, while another part of the world may operate on a standard of X.25 for network protocols. Similarly, certain standard application packages may not be available throughout the world, or support by a vendor may be not available in all geographies, making it impossible to standardize global on a particular vendor's technology.

The important thing is that security technology standards, whether region-specific or global, must support the applicable global or region-specific security policies

6. Policy approval

6.1 Governing Committee and Working Committee

Whether global or regional in scope, in order for your organization to implement information security policies, an approval structure must exist. Typically, this structure will be in the form of a committee representing the senior level management. Usually the committee will be chaired by the senior Information Security manager, with senior managers from various functional organizations participating as active members.

Since senior managers are frequently too busy to devote a high level of participation, the committee may be structured in two layers: 1) a governing committee, and 2) a working committee. In any case, it is critical to have all parts of the organization represented, including Information Technology, Legal, Personnel, as well as operating organizations.

Committee members on either level of the committee must be empowered to represent their organization in defining policy and resolving issues. The main functions of the committees are the following:

- Creating, vetting and approving the initial set of security policies and procedures.
- Revising the security policies and procedures to meet evolving needs.
- Approving requests for compliance exceptions to the policies and procedures. It is inevitable that the need for approved exceptions will arise, as the policies will not make sense in all situations, and as some organizations will face valid business reasons to delay full compliance.

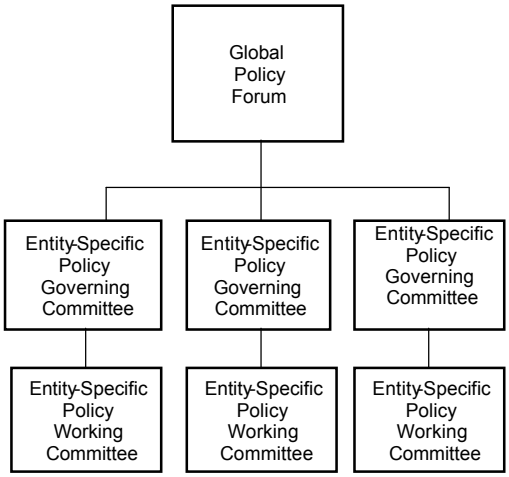
6.2 Regional Information Security Policy Approval Process

For regional information security policy to be approved is relatively simple. The Regional Security Working Committee drafts the language, vets it throughout the represented organizations, agrees on a consensus policy wording, and submits it to the Governing Security Committee for Approval. The Governing Committee may approve the policy or revision, reject it, or send it back to the Working Committee for clarification or rewording.

For a global security policy to be approved is more complicated.

Policy approval committee structure

Below is a structure that can be deployed to manage the process of developing and maintaining policies in a global organization, as well as to grant policy exceptions and variances.



If your organization is global, and you have the need for a tiered policy structure as described in this paper, this structure parallels the policy organization described in Section 6 above. Each box is described below:

Global Policy Forum

The Global Policy Forum consists of representatives from each of the Regional Policy Governing Committees, and exists to approve global policies or revisions to policies submitted to it by one or more of the Regional Policy Governing Committees. When there is a conflict between regional and global policy issues, this structure resolves the difference. The Forum will probably meet on a quarterly basis, ideally in person, but more likely, by video or audio conference.

Regional Policy Governing Committee

Each region with a set of region-specific policies will require its own Policy Governing Committee, to approve new policies, changes to policies, and to name a representative to the Global Policy Forum. The Regional Policy Governing Committee should be made up of senior managers from major divisions. It will meet monthly, or as needed based on submissions from the working committee.

A special case of a Regional Policy Governing Committee is responsible for the central organization's specific policies.

Regional Policy Working Committee

Each Region will have a working committee that does the actual policy writing, reviewing of alternate language, and submission of recommended policy changes to its Governing Committee. This committee is also empowered to approve policy exceptions that may be submitted by various organizations. The committee is made up of managers from organizations throughout the region. Representation should include the Region's legal, HR, and Audit functions, as well as operational and staff organizations.

The Working Committee should meet monthly, and submit any policy changes or additions to the governing committee for final approval.

6.3 Other considerations

A number of other considerations exist in effectively managing global information security policies. Some of those include the following.

Awareness, Education and Training

Globally, existing and new employees need to be aware of the information policies that affect them and govern acceptable behavior. This is not a static one-time requirement, since policies will be change over time. It is a significant task to communicate policies effectively throughout a global organization. Multiple languages may be necessary for training materials.

It is important to ensure that Awareness, Education and Training programs reach contractors, temporary workers, and consultants as well as employees, depending on the degree to which these individuals are exposed to sensitive information.

Grace Period for Compliance

In the case of global policies, a phased rollout to regions is probably advisable, especially if the policies need ratification by regional boards of directors or other management structures

Inevitably, when new policies are implemented, or policies are changed, compliance to the policy will not be consistent or universal immediately. A good way to deal with this is to grant a grace period for compliance. At the end of the period, a compliance survey should be performed. One way to facilitate this is to do a self-assessment at two levels, one at the managerial level, and another at the staff level. Then, a gap assessment will determine the work necessary to achieve compliance.

In any case, if you are about to tackle the problem of information security policy in a global organization, good luck! It is a difficult problem and will probably take at least a year to accomplish.

7. References

Merriam Webster New Collegiate Dictionary. Merriam Webster, Inc. 1993

Vallabhaneni, S. Rao and Vallabhaneni, Devi. CISSP Examination Textbooks, Volume1: Theory. SRV Publications. 2002. 152-154

King, C. M., Dalton, C. E., & Osmanoglu, T. E. Security Architecture: Design, Deployment and Operations, Osborne/McGraw-Hill. 2001. 2-7, 27-30, 79-80

Information Security Policy World. The Information Security Policies / Computer Security Policies Directory. 2001
http://www.information-security-policies-and-standards.com/

IT Security Policies & Network Group. IT Security Policies, Network Security Policies & Effective Delivery. 2001.
http://www.network-and-it-security-policies.com/

ISO 17799 Information Security Group. The ISO 17799 Directory. 2002
http://www.iso-17799.com/index.htm

RUsecure Information Security. RUsecure Information Security Policies. 2002
http://www.information-security-policies.com/

Security Risk associates. Security Policies & Baseline Standards: Effective Implementation. 2001
http://www.security.kirion.net/securitypolicy/

The SANS Institute. The SANS Security Policy Project. 2001
http://www.sans.org/newlook/resources/policies/policies.htm - template